determine decryption key pattern code string
Terms used: determine decryption key pattern code string

Sort results by: relevance | Save results to a Binder | Refine these results with Ad
Display results: expanded form | Open results in a new window | Try this search in The ACM C

Results 1 - 20 of 63 Result page: 1 2 3 4 next >>

1 Key management for encrypted broadcast
Avishai Wool
May 2000 ACM Transactions on Information and System Security (TISSEC), Volume 3 Issue 2
Publisher: ACM
Full text available: pdf(220.36 KB) Additional Information: full citation, abstract, references, index terms
Bibliometrics: Downloads (6 Weeks): 8, Downloads (12 Months): 130, Citation Count: 0
We consider broadcast applications where the transmissions need to be encrypted, such as direct broadcast digital TV networks or Internet multicast. In these applications the number of encrypted TV programs may be very large, but the secure memory capacity ...
Keywords: conditional access, pay-per-view

2 On the computational soundness of cryptographically masked flows
Peeter Laud
January 2008 POPL '08: Proceedings of the 35th annual ACM SIGPLAN-SIGACT symposium on Principles of programming languages
Publisher: ACM
Full text available: pdf(288.74 KB) Additional Information: full citation, abstract, references, index terms
Bibliometrics: Downloads (6 Weeks): 9, Downloads (12 Months): 110, Citation Count: 1
To speak about the security of information flow in programs employing cryptographic operations, definitions based on computational indistinguish ability of distributions over program states have to be used. These definitions, as well as the accompanying ...
Keywords: computational soundness, cryptographically masked flows, encryption, secure information flow

3 On the computational soundness of cryptographically masked flows
Peeter Laud
January 2008 ACM SIGPLAN Notices, Volume 43 Issue 1
Publisher: ACM
Full text available: pdf(288.74 KB) Additional Information: full citation, abstract, references, index terms
Bibliometrics: Downloads (6 Weeks): 9, Downloads (12 Months): 110, Citation Count: 1

To speak about the security of information flow in programs employing cryptographic operations, definitions based on computational indistinguish ability of distributions over program states have to be used. These definitions, as well as the accompanying ...

Keywords: computational soundness, cryptographically masked flows, encryption, secure information flow

4 A graph theoretic framework for preventing the wormhole attack in wireless ad hoc networks

Radha Poovendran, Loukas Lazos
January 2007 Wireless Networks, Volume 13 Issue 1
Publisher: Kluwer Academic Publishers
Full text available: pdf(1.37 MB) Additional Information: full citation, abstract, references, index terms

Bibliometrics: Downloads (6 Weeks): 21, Downloads (12 Months): 321, Citation Count: 4

Wireless ad hoc networks are envisioned to be randomly deployed in versatile and potentially hostile environments. Hence, providing secure and uninterrupted communication between the un-tethered network nodes becomes a critical problem. In this paper, ...

Keywords: geometric random graphs, security, wireless ad hoc networks, wormhole attack

5 Evading network anomaly detection systems: formal reasoning and practical techniques

Prahlad Fogla, Wenke Lee
October 2006 CCS '06: Proceedings of the 13th ACM conference on Computer and communications security
Publisher: ACM
Full text available: pdf(288.16 KB) Additional Information: full citation, abstract, references, index terms

Bibliometrics: Downloads (6 Weeks): 30, Downloads (12 Months): 413, Citation Count: 2

Attackers often try to evade an intrusion detection system (IDS) when launching their attacks. There have been several published studies in evasion attacks, some with available tools, in the research community as well as the "hackers" community. Our ...

Keywords: anomaly detection, mimicry attack, polymorphic blending attack

6 Privacy enhanced cellular access security

Geir M. Køien
September 2005 WiSe '05: Proceedings of the 4th ACM workshop on Wireless security
Publisher: ACM
Full text available: pdf(230.28 KB) Additional Information: full citation, abstract, references, index terms

Bibliometrics: Downloads (6 Weeks): 5, Downloads (12 Months): 153, Citation Count: 1

The 3G cellular access security architectures do not provide satisfactorily user privacy and fail to fully include all three principal entities involved in the security context. In this paper we propose a beyond-3G Privacy Enhanced 3-Way Authentication ...

Keywords: access security, entity authentication, wireless privacy

7 Searchable symmetric encryption: improved definitions and efficient constructions
Reza Curtmola, Juan Garay, Seny Kamara, Rafail Ostrovsky
October 2006 CCS '06: Proceedings of the 13th ACM conference on Computer and communications security
Publisher: ACM
Full text available: pdf(682.40 KB) Additional Information: full citation, abstract, references, index terms
Bibliometrics: Downloads (6 Weeks): 29, Downloads (12 Months): 198, Citation Count: 1
Searchable symmetric encryption (SSE) allows a party to outsource the storage of its data to another party (a server) in a private manner, while maintaining the ability to selectively search over it. This problem has been the focus of active research ...
Keywords: multi-user, searchable encryption, searchable symmetric encryption, security definitions

8 Validating a Web service security abstraction by typing
Andrew D. Gordon, Riccardo Pucella
November 2002 XMLSEC '02: Proceedings of the 2002 ACM workshop on XML security
Publisher: ACM
Full text available: pdf(210.31 KB) Additional Information: full citation, abstract, references, cited by, index terms
Bibliometrics: Downloads (6 Weeks): 13, Downloads (12 Months): 161, Citation Count: 10
An XML web service is, to a first approximation, an RPC service in which requests and responses are encoded in XML as SOAP envelopes, and transported over HTTP. We consider the problem of authenticating requests and responses at the SOAP-level, rather ...
Keywords: Web services, authentication, remote procedure call, type systems

9 Web customization using behavior-based remote executing agents
Eugene Hung, Joseph Pasquale
May 2004 WWW '04: Proceedings of the 13th international conference on World Wide Web
Publisher: ACM
Full text available: pdf(128.60 KB) Additional Information: full citation, abstract, references, cited by, index terms
Bibliometrics: Downloads (6 Weeks): 6, Downloads (12 Months): 56, Citation Count: 1
ReAgents are remotely executing agents that customize Web browsing for non-standard clients. A reAgent is essentially a one-shot" mobile agent that acts as an extension of a client dynamically launched by the client to run on its behalf at a remote more ...
Keywords: dynamic deployment, remote agents, web customization

10 A processing model for the optimal querying of encrypted XML documents in XQuery
Tao-Ku Chang, Gwan-Hwan Hwang
March 2007 ADC '07: Proceedings of the eighteenth conference on Australasian database - Volume 63, Volume 63
Publisher: Australian Computer Society, Inc.
Full text available: pdf(228.13 KB) Additional Information: full citation, abstract, references
Bibliometrics: Downloads (6 Weeks): 1, Downloads (12 Months): 82, Citation Count: 0
XQuery is a powerful and convenient language that is designed for querying the data in

XML documents. In this paper, we address how to optimally query encrypted XML documents using XQuery, with the key point being how to eliminate redundant decryption ...

Keywords: DSL, XML, XQuery, database, security

11 Privacy preserving error resilient dna searching through oblivious automata

Juan Ramón Troncoso-Pastoriza, Stefan Katzenbeisser, Mehmet Celik

October 2007 CCS '07: Proceedings of the 14th ACM conference on Computer and communications security

Publisher: ACM

Full text available: pdf(491.59 KB) Additional Information: full citation, abstract, references, index terms

Bibliometrics: Downloads (6 Weeks): 19, Downloads (12 Months): 168, Citation Count: 0

Human Desoxyribo-Nucleic Acid (DNA) sequences offer a wealth of information that reveal, among others, predisposition to various diseases and paternity relations. The breadth and personalized nature of this information highlights the need for privacy-preserving ...

Keywords: approximate matching, bioinformatics, dna sarch, finite automata, homomorphic encryption, levenshtein distance, secure multiparty computation

12 Access control to people location information

Urs Hengartner, Peter Steenkiste

November 2005 ACM Transactions on Information and System Security (TISSEC), Volume 8 Issue 4

Publisher: ACM

Full text available: pdf(356.85 KB) Additional Information: full citation, abstract, references, index terms, review

Bibliometrics: Downloads (6 Weeks): 34, Downloads (12 Months): 251, Citation Count: 1

Ubiquitous computing uses a variety of information for which access needs to be controlled. For instance, a person's current location is a sensitive piece of information that only authorized entities should be able to learn. Several challenges arise ...

Keywords: Certificates, DSA, RSA, SPKI/SDSI, credential discovery, delegation, location, privacy, trust

13 Private inference control

David Woodruff, Jessica Staddon

October 2004 CCS '04: Proceedings of the 11th ACM conference on Computer and communications security

Publisher: ACM

Full text available: pdf(269.55 KB) Additional Information: full citation, abstract, references, cited by, index terms

Bibliometrics: Downloads (6 Weeks): 11, Downloads (12 Months): 87, Citation Count: 2

Access control can be used to ensure that database queries pertaining to sensitive information are not answered. This is not enough to prevent users from learning sensitive information though, because users can combine non-sensitive information to discover ...

Keywords: inference control, oblivious transfer, private information retrieval

14 Verifying policy-based security for web services
Karthikeyan Bhargavan, Cédric Fournet, Andrew D. Gordon
October 2004 CCS '04: Proceedings of the 11th ACM conference on Computer and communications security
Publisher: ACM
Full text available: pdf(269.16 KB) Additional Information: full citation, abstract, references, cited by, index terms
Bibliometrics: Downloads (6 Weeks): 10, Downloads (12 Months): 268, Citation Count: 8
WS-SecurityPolicy is a declarative configuration language for driving web services security mechanisms. We describe a formal semantics for WS-SecurityPolicy, and propose a more abstract link language for specifying the security goals of web services ...
Keywords: XML security, pi calculus, web services

15 Polymorphic worm detection and defense: system design, experimental methodology, and data resources
Jisheng Wang, Ihab Hamadeh, George Kesidis, David J. Miller
September 2006 LSAD '06: Proceedings of the 2006 SIGCOMM workshop on Large-scale attack defense
Publisher: ACM
Full text available: pdf(130.95 KB) Additional Information: full citation, abstract, references, index terms
Bibliometrics: Downloads (6 Weeks): 10, Downloads (12 Months): 151, Citation Count: 1
The polymorphic variety of Internet worms presents a formidable challenge to network intrusion detection and methods designed to extract payload signatures for worm containment. Recently, several systems, including Earlybird and Polygraph, have been ...
Keywords: intrusion detection system, network anomaly detection, polymorphic worms, worm signature extraction

16 Data-centric security: role analysis and role typestates
Vugranam C. Sreedhar
June 2006 SACMAT '06: Proceedings of the eleventh ACM symposium on Access control models and technologies
Publisher: ACM
Full text available: pdf(270.98 KB) Additional Information: full citation, abstract, references, index terms
Bibliometrics: Downloads (6 Weeks): 6, Downloads (12 Months): 101, Citation Count: 0
In J2EE and .NET roles are assigned to methods using external configuration files, called the deployment descriptors. Assigning roles to methods, although conceptually simple, in practice it is quite complicated. For instance, in order for a deployer ...
Keywords: RBAC, role analysis, role escape analysis, role typestates

17 The faithfulness of abstract protocol analysis: message authentication
Joshua D. Guttman, F. Javier Thayer, Lenore D. Zuck
November 2001 CCS '01: Proceedings of the 8th ACM conference on Computer and Communications Security
Publisher: ACM
Full text available: pdf(259.03 KB) Additional Information: full citation, abstract, references, cited by, index

terms

Bibliometrics: Downloads (6 Weeks): 4, Downloads (12 Months): 35, Citation Count: 8

Dolev and Yao initiated an approach to studying cryptographic protocols which abstracts from possible problems with the cryptography so as to focus on the structural aspects of the protocol. Recent work in this framework has developed easily applicable ...

18 Display-only file server: a solution against information theft due to insider attack

Yang Yu, Tzi-cker Chiueh

October 2004 DRM '04: Proceedings of the 4th ACM workshop on Digital rights management

Publisher: ACM

Full text available: pdf(311.80 KB) Additional Information: full citation, abstract, references, index terms

Bibliometrics: Downloads (6 Weeks): 20, Downloads (12 Months): 158, Citation Count: 1

Insider attack is one of the most serious cybersecurity threats to corporate America. Among all insider threats, information theft is considered the most damaging in terms of potential financial loss. Moreover, it is also especially difficult to detect ...

Keywords: access, digital rights management, information theft, insider attack

19 Watermarking cyberspace

Hal Berghel

November 1997 Communications of the ACM, Volume 40 Issue 11

Publisher: ACM

Full text available: pdf(1.70 MB) Additional Information: full citation, cited by, index terms

Bibliometrics: Downloads (6 Weeks): 5, Downloads (12 Months): 64, Citation Count: 3

20 Randomized instruction set emulation

Elena Gabriela Barrantes, David H. Ackley, Stephanie Forrest, Darko Stefanović

February 2005 ACM Transactions on Information and System Security (TISSEC), Volume 8 Issue 1

Publisher: ACM

Full text available: pdf(374.44 KB) Additional Information: full citation, abstract, references, cited by, index terms

Bibliometrics: Downloads (6 Weeks): 15, Downloads (12 Months): 177, Citation Count: 4

Injecting binary code into a running program is a common form of attack. Most defenses employ a "guard the doors" approach, blocking known mechanisms of code injection. *Randomized instruction set emulation* (RISE) is a complementary ...

Keywords: Automated diversity, randomized instruction sets, software diversity